18. State and prove the law of Quadratic Reciprocity.

19. Write down the algorithm for finding discrete logs in finite fields.

20. Define Fermat factorization method using it find the factor of 200819.

Shanmuga Industries Arts & Science College T.V.Malai

APRIL/MAY 2024

DEMA44A/GEMA44A — NUMBER THEORY AND CRYPTOGRAPHY

Time : Three hours Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

1. Define the Euler phi-function.

2. Write any two properties on congruences.

3. What do you mean by cryptosystem?

4. What is affine enciphering transformations?

5. Find all the quadratic residues and non residues of F_{11}.

6. What is reciprocity?

7. Define enciphering key and deciphering key.

8. Expand the term RSA.

9. Define Pseudoprime and give an example which is not a pseudo prime.

10. Find a proper divisor of 91, using rho method.

SECTION B — (5 × 5 = 25 marks)

Answer ALL questions.

11. (a) Express 7 as a linear combination of 1547 and 560.

Or

(b) Obtain the factor $3^{12}-1$.

12. (a) In the 27 - letter alphabet (with blank space = 26) use the affine enciphering transformation with key a = 13, b = 9 encipher the message "HELP ME".

Or

(b) Using the matrix $A=\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix}\in M_2(Z/26Z)$ decipher the ciphertext "FWMDIQ".

13. (a) Prove that $(a+b)^p=a^p+b^p$ in any field of characteristic P.

Or

(b) Determine whether 7411 is a residue modulo the prime 9283.

14. (a) Explain the Diffie-Hellman key exchange system.

Or

(b) Find the discrete log of 28 to the base 2 in F_{37}^* using silver-Pohlig-Hellmon algorithm (2 is a generator of F_{37}^*).

15. (a) Show that a Carmichael number must be the product of atleast three distinct primes.

Or

(b) Factor 4087 using $f(x)=x^2+x+1$ with $x_0=2$.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

16. State and prove Chinese Remainder Theorem.

17. Let $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in M_2(Z/NZ)$ and set D = ad-bc, then prove that the following are equivalent.

(a) $g.c.d(D,N)=1$.

(b) A has an inverse matrix

(c) If x and y are note both 0 in Z/NZ, then $A\begin{pmatrix}x\\ y\end{pmatrix}\neq\begin{pmatrix}0\\ 0\end{pmatrix}$.

(d) A gives a 1-to-1 correspondence of $(Z/NZ)^2$ with itself.